Networks Lab Assignment 1 Report

Dadi Sasank Kumar (22CS10020)

January 17, 2025

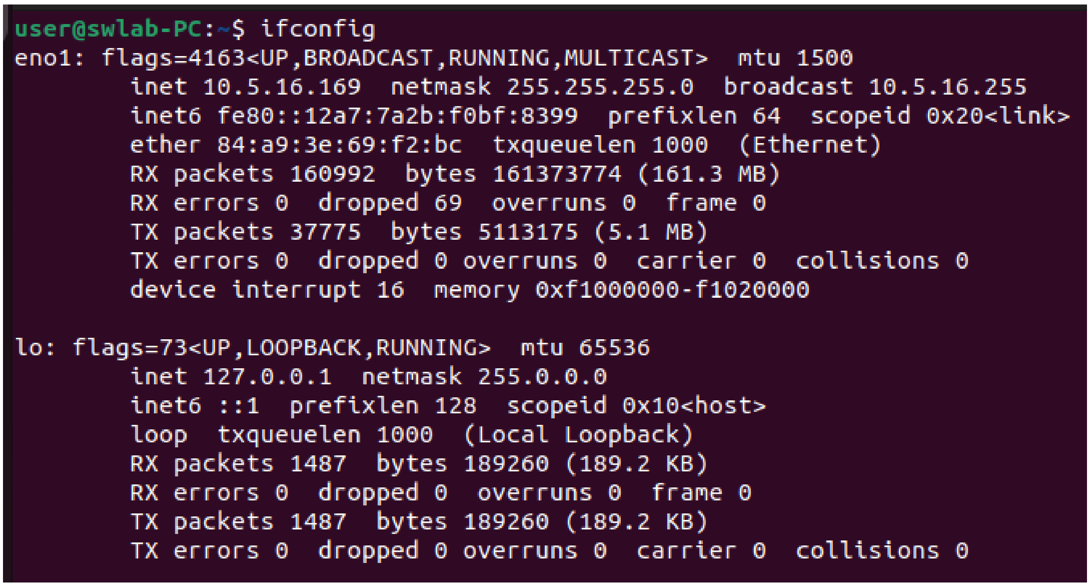
Part 1: Networking Tools

1 Task 1: Find the IP Address, Subnet Mask, and Network ID

Using the `ifconfig` command, we identified the following:

- **IP Address of the Machine:** `10.5.16.169`
- **Subnet Mask:** `255.255.255.0`
- **Network ID:** `10.5.16.0`

Screenshot of the output:



```
user@swlab-PC:~$ ifconfig
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.5.16.169  netmask 255.255.255.0  broadcast 10.5.16.255
        inet6 fe80::12a7:7a2b:f0bf:8399  prefixlen 64  scopeid 0x20<link>
        ether 84:a9:3e:69:f2:bc  txqueuelen 1000  (Ethernet)
        RX packets 160992  bytes 161373774 (161.3 MB)
        RX errors 0  dropped 69  overruns 0  frame 0
        TX packets 37775  bytes 5113175 (5.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16  memory 0xf1000000-f1020000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1487  bytes 189260 (189.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1487  bytes 189260 (189.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

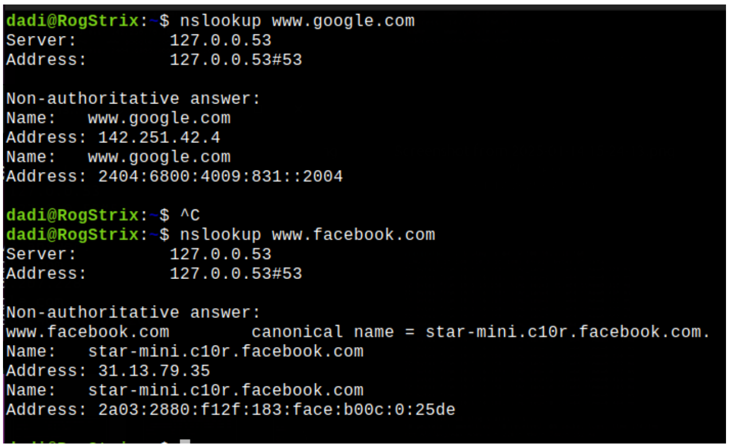
Figure 1: Output of `ifconfig` showing IP address, subnet mask, and network ID.

2 Task 2: Resolve Domain Names using `nslookup`

Using `nslookup`, the IP addresses for `www.google.com` and `www.facebook.com` were obtained:

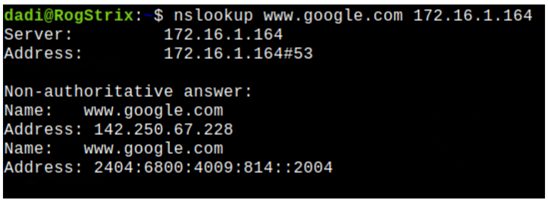
- **IP Address of www.google.com:** 142.251.42.4
- **IP Address of www.facebook.com:** 31.13.79.35

When the DNS server address was changed to 172.16.1.164, 172.16.1.180, 172.16.1.165, and 172.16.1.166, the IP address of www.google.com was observed to change. This behavior is due to the load-balancing mechanisms used by DNS servers. These mechanisms ensure that traffic is distributed efficiently across multiple servers, improving performance, reliability, and redundancy.



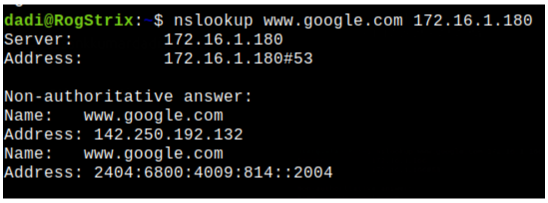
```
dadi@RogStrix:~$ nslookup www.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.251.42.4
Name:   www.google.com
Address: 2404:6800:4009:831::2004

dadi@RogStrix:~$ ^C
dadi@RogStrix:~$ nslookup www.facebook.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.facebook.com        canonical name = star-mini.c10r.facebook.com.
Name:   star-mini.c10r.facebook.com
Address: 31.13.79.35
Name:   star-mini.c10r.facebook.com
Address: 2a03:2880:f12f:183:face:b00c:0:25de
```

Figure 2: IP address associated with www.google.com and www.facebook.com



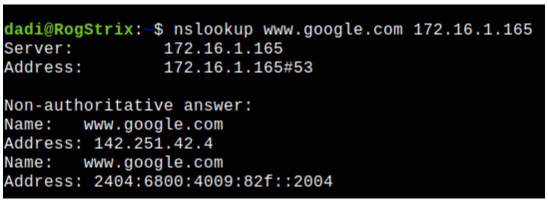
```
dadi@RogStrix:~$ nslookup www.google.com 172.16.1.164
Server:         172.16.1.164
Address:        172.16.1.164#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.67.228
Name:   www.google.com
Address: 2404:6800:4009:814::2004
```

Figure 3: IP address of www.google.com with DNS address 172.16.1.164



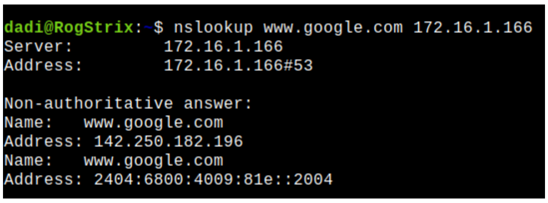
```
dadi@RogStrix:~$ nslookup www.google.com 172.16.1.180
Server:         172.16.1.180
Address:        172.16.1.180#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.192.132
Name:   www.google.com
Address: 2404:6800:4009:814::2004
```

Figure 4: IP address of www.google.com with DNS address 172.16.1.180



```
dadi@RogStrix:~$ nslookup www.google.com 172.16.1.165
Server:         172.16.1.165
Address:        172.16.1.165#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.251.42.4
Name:   www.google.com
Address: 2404:6800:4009:82f::2004
```

Figure 5: IP address of www.google.com with DNS address 172.16.1.165



```
dadi@RogStrix:~$ nslookup www.google.com 172.16.1.166
Server:         172.16.1.166
Address:        172.16.1.166#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.182.196
Name:   www.google.com
Address: 2404:6800:4009:81e::2004
```

Figure 6: IP address of www.google.com with DNS address 172.16.1.166

DNS	IP address
172.16.1.164	142.250.67.228
172.16.1.180	142.250.192.132
172.16.1.165	142.251.42.4
172.16.1.166	142.250.182.196

3 Task 3: Ping Command with Different Packet Sizes

Using the `ping` command, packets were sent to a friend's machine with varying sizes:

- Friend's IP Address: `10.5.16.152`
- Packet Sizes: 64, 128, 512 bytes.
- Timeout: 100ms.

Results Table

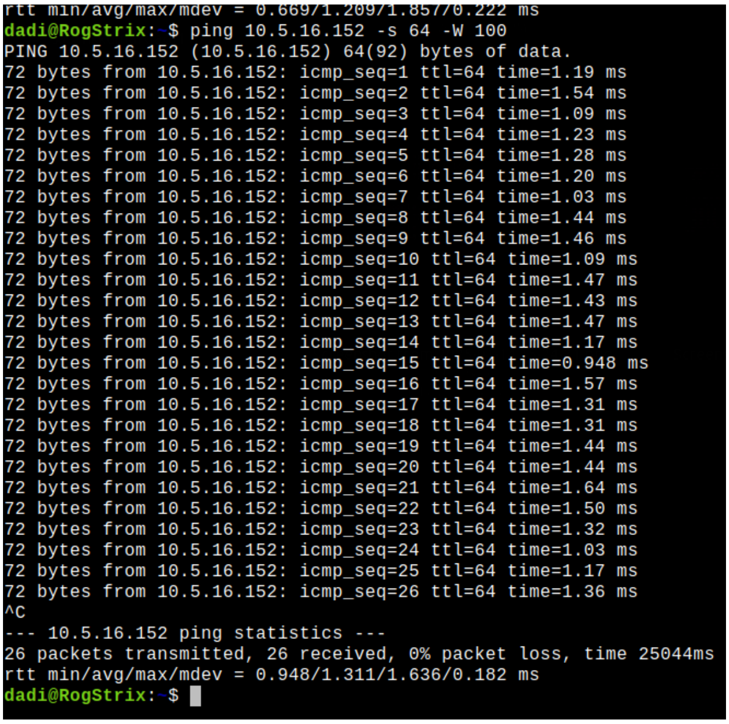
The results of the ping command with varying packet sizes are summarized below:

Packet Size (bytes)	Packet Loss (%)	Round-Trip Time (min/avg/max/stddev)
64	0	0.948 / 1.311 / 1.636/ 0.182
128	0	1.025 / 1.261 / 1.513/ 0.161
512	0	1.203 / 1.404 / 1.674 / 0.122

Table 1: Summary of `ping` results for different packet sizes.

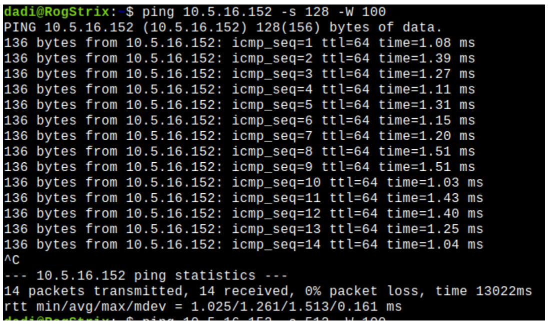
Screenshots

The following images show the ping command outputs for each packet size:



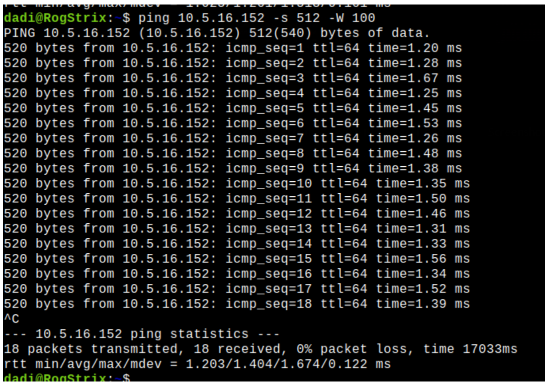
```
rtt min/avg/max/mdev = 0.669/1.209/1.857/0.222 ms
dadi@RogStrix:~$ ping 10.5.16.152 -s 64 -W 100
PING 10.5.16.152 (10.5.16.152) 64(92) bytes of data.
72 bytes from 10.5.16.152: icmp_seq=1 ttl=64 time=1.19 ms
72 bytes from 10.5.16.152: icmp_seq=2 ttl=64 time=1.54 ms
72 bytes from 10.5.16.152: icmp_seq=3 ttl=64 time=1.09 ms
72 bytes from 10.5.16.152: icmp_seq=4 ttl=64 time=1.23 ms
72 bytes from 10.5.16.152: icmp_seq=5 ttl=64 time=1.28 ms
72 bytes from 10.5.16.152: icmp_seq=6 ttl=64 time=1.20 ms
72 bytes from 10.5.16.152: icmp_seq=7 ttl=64 time=1.03 ms
72 bytes from 10.5.16.152: icmp_seq=8 ttl=64 time=1.44 ms
72 bytes from 10.5.16.152: icmp_seq=9 ttl=64 time=1.46 ms
72 bytes from 10.5.16.152: icmp_seq=10 ttl=64 time=1.09 ms
72 bytes from 10.5.16.152: icmp_seq=11 ttl=64 time=1.47 ms
72 bytes from 10.5.16.152: icmp_seq=12 ttl=64 time=1.43 ms
72 bytes from 10.5.16.152: icmp_seq=13 ttl=64 time=1.47 ms
72 bytes from 10.5.16.152: icmp_seq=14 ttl=64 time=1.17 ms
72 bytes from 10.5.16.152: icmp_seq=15 ttl=64 time=0.948 ms
72 bytes from 10.5.16.152: icmp_seq=16 ttl=64 time=1.57 ms
72 bytes from 10.5.16.152: icmp_seq=17 ttl=64 time=1.31 ms
72 bytes from 10.5.16.152: icmp_seq=18 ttl=64 time=1.31 ms
72 bytes from 10.5.16.152: icmp_seq=19 ttl=64 time=1.44 ms
72 bytes from 10.5.16.152: icmp_seq=20 ttl=64 time=1.44 ms
72 bytes from 10.5.16.152: icmp_seq=21 ttl=64 time=1.64 ms
72 bytes from 10.5.16.152: icmp_seq=22 ttl=64 time=1.50 ms
72 bytes from 10.5.16.152: icmp_seq=23 ttl=64 time=1.32 ms
72 bytes from 10.5.16.152: icmp_seq=24 ttl=64 time=1.03 ms
72 bytes from 10.5.16.152: icmp_seq=25 ttl=64 time=1.17 ms
72 bytes from 10.5.16.152: icmp_seq=26 ttl=64 time=1.36 ms
^C
--- 10.5.16.152 ping statistics ---
26 packets transmitted, 26 received, 0% packet loss, time 25044ms
rtt min/avg/max/mdev = 0.948/1.311/1.636/0.182 ms
dadi@RogStrix:~$
```

Figure 7: Ping output for 64-byte packets.



```
dadi@RogStrix:~$ ping 10.5.16.152 -s 128 -W 100
PING 10.5.16.152 (10.5.16.152) 128(156) bytes of data.
136 bytes from 10.5.16.152: icmp_seq=1 ttl=64 time=1.08 ms
136 bytes from 10.5.16.152: icmp_seq=2 ttl=64 time=1.39 ms
136 bytes from 10.5.16.152: icmp_seq=3 ttl=64 time=1.27 ms
136 bytes from 10.5.16.152: icmp_seq=4 ttl=64 time=1.11 ms
136 bytes from 10.5.16.152: icmp_seq=5 ttl=64 time=1.31 ms
136 bytes from 10.5.16.152: icmp_seq=6 ttl=64 time=1.15 ms
136 bytes from 10.5.16.152: icmp_seq=7 ttl=64 time=1.20 ms
136 bytes from 10.5.16.152: icmp_seq=8 ttl=64 time=1.51 ms
136 bytes from 10.5.16.152: icmp_seq=9 ttl=64 time=1.51 ms
136 bytes from 10.5.16.152: icmp_seq=10 ttl=64 time=1.03 ms
136 bytes from 10.5.16.152: icmp_seq=11 ttl=64 time=1.43 ms
136 bytes from 10.5.16.152: icmp_seq=12 ttl=64 time=1.40 ms
136 bytes from 10.5.16.152: icmp_seq=13 ttl=64 time=1.25 ms
136 bytes from 10.5.16.152: icmp_seq=14 ttl=64 time=1.04 ms
^C
--- 10.5.16.152 ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 13022ms
rtt min/avg/max/mdev = 1.025/1.261/1.513/0.161 ms
dadi@RogStrix:~$ ping 10.5.16.152 -s 512 -W 100
```

Figure 8: Ping output for 128-byte packets.



```
rtt min/avg/max/mdev = 1.025/1.261/1.513/0.161 ms
dadi@RogStrix:~$ ping 10.5.16.152 -s 512 -W 100
PING 10.5.16.152 (10.5.16.152) 512(540) bytes of data.
520 bytes from 10.5.16.152: icmp_seq=1 ttl=64 time=1.20 ms
520 bytes from 10.5.16.152: icmp_seq=2 ttl=64 time=1.28 ms
520 bytes from 10.5.16.152: icmp_seq=3 ttl=64 time=1.67 ms
520 bytes from 10.5.16.152: icmp_seq=4 ttl=64 time=1.25 ms
520 bytes from 10.5.16.152: icmp_seq=5 ttl=64 time=1.45 ms
520 bytes from 10.5.16.152: icmp_seq=6 ttl=64 time=1.53 ms
520 bytes from 10.5.16.152: icmp_seq=7 ttl=64 time=1.26 ms
520 bytes from 10.5.16.152: icmp_seq=8 ttl=64 time=1.48 ms
520 bytes from 10.5.16.152: icmp_seq=9 ttl=64 time=1.38 ms
520 bytes from 10.5.16.152: icmp_seq=10 ttl=64 time=1.35 ms
520 bytes from 10.5.16.152: icmp_seq=11 ttl=64 time=1.50 ms
520 bytes from 10.5.16.152: icmp_seq=12 ttl=64 time=1.46 ms
520 bytes from 10.5.16.152: icmp_seq=13 ttl=64 time=1.31 ms
520 bytes from 10.5.16.152: icmp_seq=14 ttl=64 time=1.33 ms
520 bytes from 10.5.16.152: icmp_seq=15 ttl=64 time=1.56 ms
520 bytes from 10.5.16.152: icmp_seq=16 ttl=64 time=1.34 ms
520 bytes from 10.5.16.152: icmp_seq=17 ttl=64 time=1.52 ms
520 bytes from 10.5.16.152: icmp_seq=18 ttl=64 time=1.39 ms
^C
--- 10.5.16.152 ping statistics ---
18 packets transmitted, 18 received, 0% packet loss, time 17033ms
rtt min/avg/max/mdev = 1.203/1.404/1.674/0.122 ms
dadi@RogStrix:~$
```

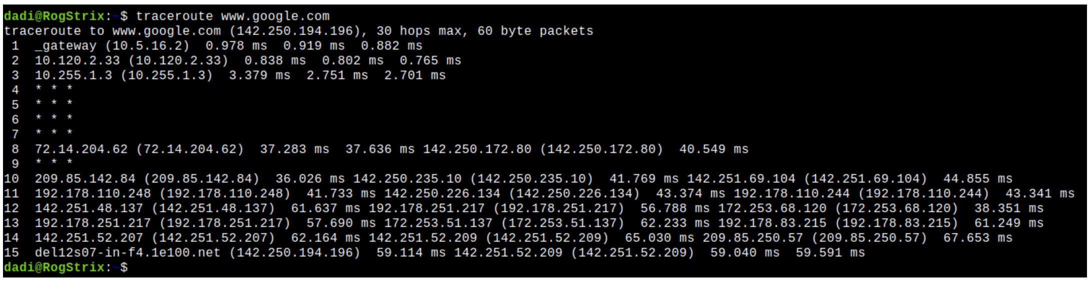
Figure 9: Ping output for 512-byte packets.

4 Task 4: Traceroute Command

Using the `traceroute` command, the path to `www.google.com` was analyzed. The number of hosts involved in the path from source to destination was counted.
Summary of Results:

- Number of Hosts: `15`
- Observed "* * *" in intermediate hops: These indicate timeouts or unreachable hosts, often caused by network policies or firewalls or TTL expiration without response

Screenshot of the output:



```
dadi@RogStrix:~$ traceroute www.google.com
traceroute to www.google.com (142.250.194.196), 30 hops max, 60 byte packets
 1  _gateway (10.5.16.2)  0.978 ms  0.919 ms  0.882 ms
 2  10.120.2.33 (10.120.2.33)  0.838 ms  0.802 ms  0.765 ms
 3  10.255.1.3 (10.255.1.3)  3.379 ms  2.751 ms  2.701 ms
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  72.14.204.62 (72.14.204.62)  37.283 ms  37.636 ms 142.250.172.80 (142.250.172.80)  40.549 ms
 9  * * *
10  209.85.142.84 (209.85.142.84)  36.026 ms 142.250.235.10 (142.250.235.10)  41.769 ms 142.251.69.104 (142.251.69.104)  44.855 ms
11  192.178.110.248 (192.178.110.248)  41.733 ms 142.250.226.134 (142.250.226.134)  43.374 ms 192.178.110.244 (192.178.110.244)  43.341 ms
12  142.251.48.137 (142.251.48.137)  61.637 ms 192.178.251.217 (192.178.251.217)  56.788 ms 172.253.68.120 (172.253.68.120)  38.351 ms
13  192.178.251.217 (192.178.251.217)  57.690 ms 172.253.51.137 (172.253.51.137)  62.233 ms 192.178.83.215 (192.178.83.215)  61.249 ms
14  142.251.52.207 (142.251.52.207)  62.164 ms 142.251.52.209 (142.251.52.209)  65.030 ms 209.85.250.57 (209.85.250.57)  67.653 ms
15  del12s07-in-f4.1e100.net (142.250.194.196)  59.114 ms 142.251.52.209 (142.251.52.209)  59.040 ms  59.591 ms
dadi@RogStrix:~$
```

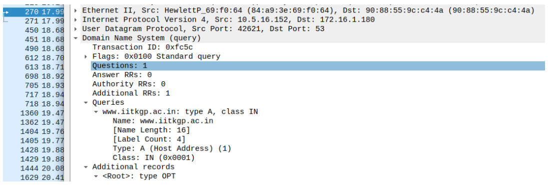
Figure 10: Output of `traceroute` for `www.google.com`.

Part 2: Packet Analysis

1. DNS Packets Analysis

- **DNS Query/Response Protocol:** UDP
- **Source IP Address of DNS Query:** 10.5.16.152
- **Destination IP Address of DNS Query:** 172.16.1.180
- **Number of DNS Queries Sent:** 69
- **DNS Server Replying with IP Address:** 172.16.1.180

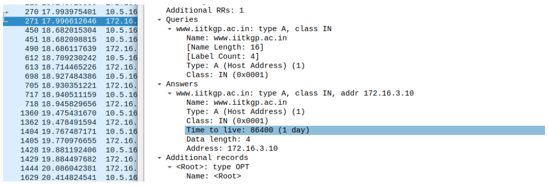
- **Number of DNS Servers Involved:** 1 (Not all DNS servers responded)
- **Resource Records:**



```
270 17.99
271 17.99
450 18.68
451 18.68
490 18.68
612 18.70
613 18.71
698 18.92
705 18.93
717 18.94
718 18.94
1360 19.47
1362 19.47
1404 19.76
1405 19.77
1428 19.88
1429 19.88
1444 20.08
1629 20.41
```

```
▸ Ethernet II, Src: HewlettP_69:f0:64 (84:a9:3e:69:f0:64), Dst: 90:88:55:9c:c4:4a (90:88:55:9c:c4:4a)
▸ Internet Protocol Version 4, Src: 10.5.16.152, Dst: 172.16.1.180
▸ User Datagram Protocol, Src Port: 42621, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0xfc5c
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▾ www.iitkgp.ac.in: type A, class IN
        Name: www.iitkgp.ac.in
        [Name Length: 16]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ▾ Additional records
    ▾ <Root>: type OPT
```

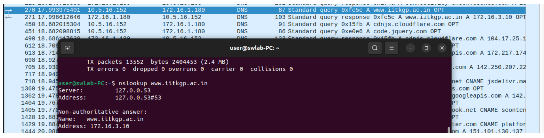
Figure 11: DNS Query



```
270 17.993975401  10.5.16
271 17.996612646  172.16.
450 18.682015304  10.5.16
451 18.682098815  10.5.16
490 18.686117639  172.16.
612 18.709230242  10.5.16
613 18.714465226  172.16.
698 18.927484386  10.5.16
705 18.930351221  172.16.
717 18.940511159  10.5.16
718 18.945829656  172.16.
1360 19.475431670  10.5.16
1362 19.478491594  172.16.
1404 19.767487171  10.5.16
1405 19.770976655  172.16.
1428 19.881192406  10.5.16
1429 19.884497682  172.16.
1444 20.086042381  172.16.
1629 20.414824541  10.5.16
```

```
    Additional RRs: 1
  ▾ Queries
    ▾ www.iitkgp.ac.in: type A, class IN
        Name: www.iitkgp.ac.in
        [Name Length: 16]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ▾ Answers
    ▾ www.iitkgp.ac.in: type A, class IN, addr 172.16.3.10
        Name: www.iitkgp.ac.in
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 86400 (1 day)
        Data length: 4
        Address: 172.16.3.10
  ▾ Additional records
    ▾ <Root>: type OPT
        Name: <Root>
```

Figure 12: DNS Response



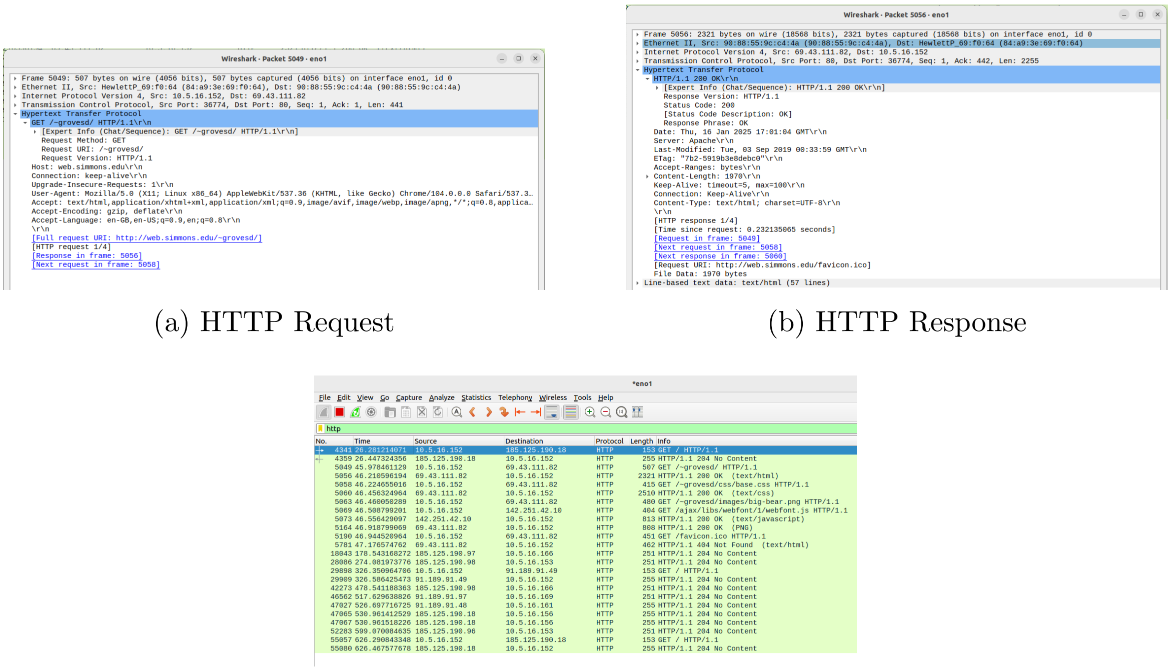
```
270 17.993975401 10.5.16.152    172.16.1.180   DNS   87 Standard query 0xfc5c A www.iitkgp.ac.in OPT
271 17.996612646 172.16.1.180   10.5.16.152    DNS  103 Standard query response 0xfc5c A www.iitkgp.ac.in A 172.16.3.10 OPT
450 18.682015304 10.5.16.152    172.16.1.180   DNS   91 Standard query 0x15fb A cdnjs.cloudflare.com OPT
451 18.682098815 10.5.16.152    172.16.1.180   DNS   86 Standard query 0xe0e6 A code.jquery.com OPT
```

```
       TX packets 13552  bytes 2404453 (2.4 MB)
       TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

user@swlab-PC:~$ nslookup www.iitkgp.ac.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.iitkgp.ac.in
Address: 172.16.3.10
```

Figure 13: nslookup response

2. Web Traffic (HTTP) Analysis

- **Number of HTTP Packets Exchanged:** 12
- **HTTP Request:** GET /˜grovesd/ HTTP/1.1
- **HTTP Response:** HTTP/1.1 200 OK (text.html)



```
▸ Frame 5049: 507 bytes on wire (4056 bits), 507 bytes captured (4056 bits) on interface eno1, id 0
▸ Ethernet II, Src: HewlettP_69:f0:64 (84:a9:3e:69:f0:64), Dst: 90:88:55:9c:c4:4a (90:88:55:9c:c4:4a)
▸ Internet Protocol Version 4, Src: 10.5.16.152, Dst: 69.43.111.82
▸ Transmission Control Protocol, Src Port: 36774, Dst Port: 80, Seq: 1, Ack: 1, Len: 441
▾ Hypertext Transfer Protocol
  ▾ GET /~grovesd/ HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET /~grovesd/ HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /~grovesd/
      Request Version: HTTP/1.1
    Host: web.simmons.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.3…
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applica…
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
    \r\n
    [Full request URI: http://web.simmons.edu/~grovesd/]
    [HTTP request 1/4]
    [Response in frame: 5056]
    [Next request in frame: 5058]
```

(a) HTTP Request

```
▸ Frame 5056: 2321 bytes on wire (18568 bits), 2321 bytes captured (18568 bits) on interface eno1, id 0
▸ Ethernet II, Src: 90:88:55:9c:c4:4a (90:88:55:9c:c4:4a), Dst: HewlettP_69:f0:64 (84:a9:3e:69:f0:64)
▸ Internet Protocol Version 4, Src: 69.43.111.82, Dst: 10.5.16.152
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 36774, Seq: 1, Ack: 442, Len: 2255
▾ Hypertext Transfer Protocol
  ▾ HTTP/1.1 200 OK\r\n
    ▸ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Thu, 16 Jan 2025 17:01:04 GMT\r\n
    Server: Apache\r\n
    Last-Modified: Tue, 03 Sep 2019 00:33:59 GMT\r\n
    ETag: "7b2-5919b3e8debc0"\r\n
    Accept-Ranges: bytes\r\n
  ▸ Content-Length: 1970\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/4]
    [Time since request: 0.232135065 seconds]
    [Request in frame: 5049]
    [Next request in frame: 5058]
    [Next response in frame: 5060]
    [Request URI: http://web.simmons.edu/favicon.ico]
    File Data: 1970 bytes
▸ Line-based text data: text/html (57 lines)
```

(b) HTTP Response

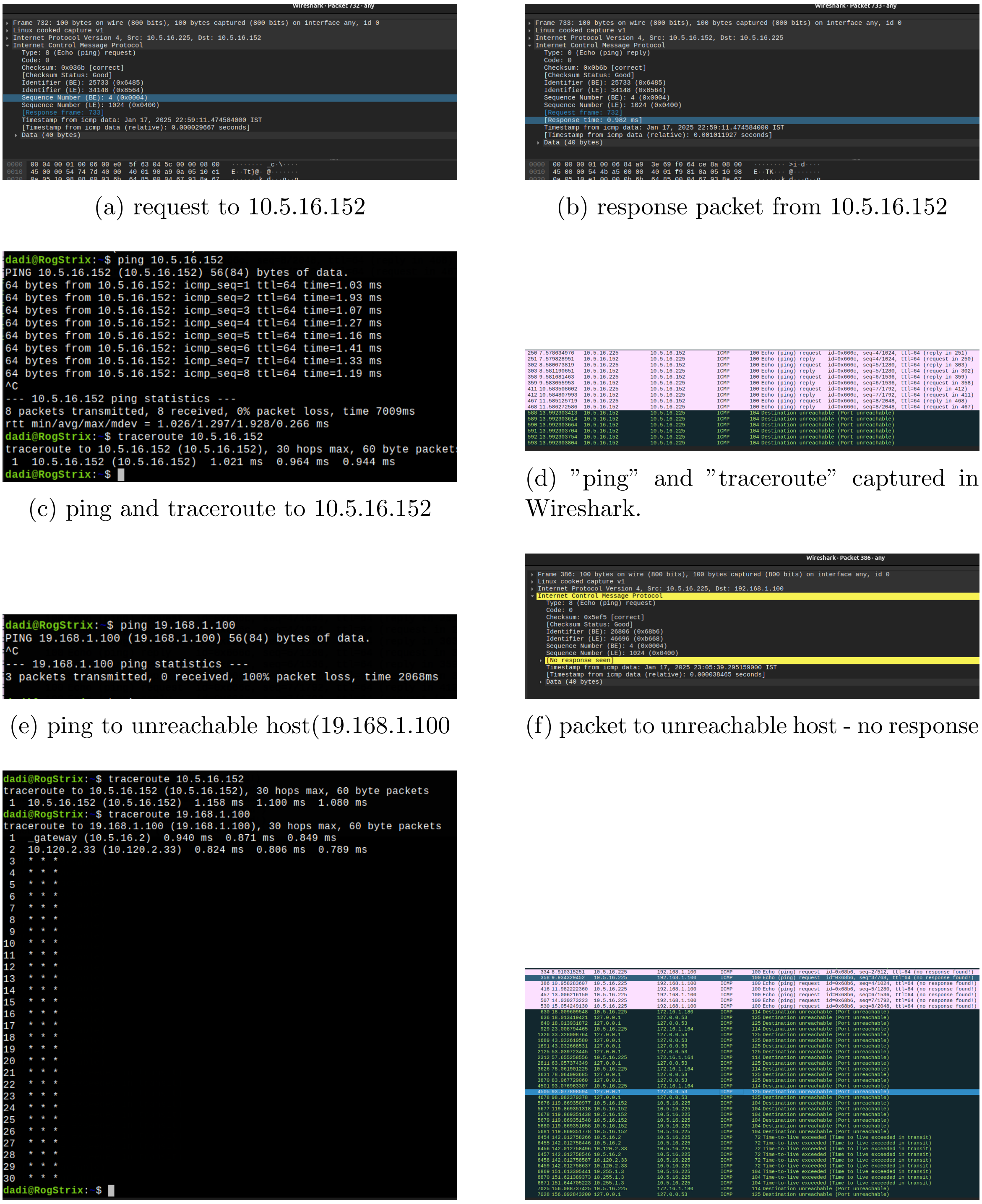
```
No.   Time         Source          Destination     Protocol Length Info
 4341 26.281214071 10.5.16.152     185.125.190.18  HTTP      153 GET / HTTP/1.1
 4359 26.447324356 185.125.190.18  10.5.16.152     HTTP      255 HTTP/1.1 204 No Content
 5049 45.978461129 10.5.16.152     69.43.111.82    HTTP      507 GET /~grovesd/ HTTP/1.1
 5056 46.210596194 69.43.111.82    10.5.16.152     HTTP     2321 HTTP/1.1 200 OK  (text/html)
 5058 46.224655016 10.5.16.152     69.43.111.82    HTTP      415 GET /~grovesd/css/base.css HTTP/1.1
 5060 46.456324964 69.43.111.82    10.5.16.152     HTTP     2510 HTTP/1.1 200 OK  (text/css)
 5063 46.460050289 10.5.16.152     69.43.111.82    HTTP      480 GET /~grovesd/images/big-bear.png HTTP/1.1
 5069 46.508799201 10.5.16.152     142.251.42.10   HTTP      404 GET /ajax/libs/webfont/1/webfont.js HTTP/1.1
 5073 46.556429097 142.251.42.10   10.5.16.152     HTTP      813 HTTP/1.1 200 OK  (text/javascript)
 5164 46.918799069 69.43.111.82    10.5.16.152     HTTP      808 HTTP/1.1 200 OK  (PNG)
 5190 46.944520964 10.5.16.152     69.43.111.82    HTTP      451 GET /favicon.ico HTTP/1.1
 5781 47.176574762 69.43.111.82    10.5.16.152     HTTP      462 HTTP/1.1 404 Not Found  (text/html)
18043 178.543168272 185.125.190.97 10.5.16.166     HTTP      251 HTTP/1.1 204 No Content
28086 274.081973776 185.125.190.98 10.5.16.153     HTTP      251 HTTP/1.1 204 No Content
29898 326.350964706 10.5.16.152    91.189.91.49    HTTP      153 GET / HTTP/1.1
29909 326.586425473 91.189.91.49   10.5.16.152     HTTP      255 HTTP/1.1 204 No Content
42273 478.541188363 185.125.190.98 10.5.16.166     HTTP      251 HTTP/1.1 204 No Content
46562 517.629638826 91.189.91.97   10.5.16.169     HTTP      251 HTTP/1.1 204 No Content
47027 526.697716725 91.189.91.48   10.5.16.161     HTTP      255 HTTP/1.1 204 No Content
47065 530.961412529 185.125.190.18 10.5.16.156     HTTP      255 HTTP/1.1 204 No Content
47067 530.961518226 185.125.190.18 10.5.16.156     HTTP      255 HTTP/1.1 204 No Content
52283 599.070084635 185.125.190.96 10.5.16.153     HTTP      251 HTTP/1.1 204 No Content
55057 626.290843348 10.5.16.152    185.125.190.18  HTTP      153 GET / HTTP/1.1
55080 626.467577678 185.125.190.18 10.5.16.152     HTTP      255 HTTP/1.1 204 No Content
```

(c) HTTP Request 3.

Figure 14: HTTP Request and Response for http://web.simmons.edu/ grovesd/.

3. ICMP Traffic (Ping/Traceroute)

- **Ping to Friend's IP:** 10.5.16.152
- **Traceroute to Friend's IP:** 10.5.16.152
- **Ping to Unreachable Host:** 192.168.1.100



```
Wireshark · Packet 732 · any
 Frame 732: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
 Linux cooked capture v1
 Internet Protocol Version 4, Src: 10.5.16.225, Dst: 10.5.16.152
 Internet Control Message Protocol
   Type: 8 (Echo (ping) request)
   Code: 0
   Checksum: 0x036b [correct]
   [Checksum Status: Good]
   Identifier (BE): 25733 (0x6485)
   Identifier (LE): 34148 (0x8564)
   Sequence Number (BE): 4 (0x0004)
   Sequence Number (LE): 1024 (0x0400)
   [Response frame: 733]
   Timestamp from icmp data: Jan 17, 2025 22:59:11.474584000 IST
   [Timestamp from icmp data (relative): 0.000029667 seconds]
  Data (40 bytes)

0000  00 04 00 01 00 06 00 e0  5f 63 04 5c 00 00 08 00   ········ _c·\····
0010  45 00 00 54 74 7d 40 00  40 01 90 a9 0a 05 10 e1   E··Tt}@· @·······
0020  0a 05 10 98 08 00 03 6b  64 85 00 04 67 93 8a 67   ·······k d···g··g
```

(a) request to 10.5.16.152

```
Wireshark · Packet 733 · any
 Frame 733: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
 Linux cooked capture v1
 Internet Protocol Version 4, Src: 10.5.16.152, Dst: 10.5.16.225
 Internet Control Message Protocol
   Type: 0 (Echo (ping) reply)
   Code: 0
   Checksum: 0x0b6b [correct]
   [Checksum Status: Good]
   Identifier (BE): 25733 (0x6485)
   Identifier (LE): 34148 (0x8564)
   Sequence Number (BE): 4 (0x0004)
   Sequence Number (LE): 1024 (0x0400)
   [Request frame: 732]
   [Response time: 0.982 ms]
   Timestamp from icmp data: Jan 17, 2025 22:59:11.474584000 IST
   [Timestamp from icmp data (relative): 0.001011927 seconds]
  Data (40 bytes)

0000  00 00 00 01 00 06 84 a9  3e 69 f0 64 ce 8a 08 00   ········ >i·d····
0010  45 00 00 54 4b a5 00 00  40 01 f9 81 0a 05 10 98   E··TK··· @·······
0020  0a 05 10 e1 00 00 0b 6b  64 85 00 04 67 93 8a 67   ·······k d···g··g
```

(b) response packet from 10.5.16.152

```
dadi@RogStrix:~$ ping 10.5.16.152
PING 10.5.16.152 (10.5.16.152) 56(84) bytes of data.
64 bytes from 10.5.16.152: icmp_seq=1 ttl=64 time=1.03 ms
64 bytes from 10.5.16.152: icmp_seq=2 ttl=64 time=1.93 ms
64 bytes from 10.5.16.152: icmp_seq=3 ttl=64 time=1.07 ms
64 bytes from 10.5.16.152: icmp_seq=4 ttl=64 time=1.27 ms
64 bytes from 10.5.16.152: icmp_seq=5 ttl=64 time=1.16 ms
64 bytes from 10.5.16.152: icmp_seq=6 ttl=64 time=1.41 ms
64 bytes from 10.5.16.152: icmp_seq=7 ttl=64 time=1.33 ms
64 bytes from 10.5.16.152: icmp_seq=8 ttl=64 time=1.19 ms
^C
--- 10.5.16.152 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7009ms
rtt min/avg/max/mdev = 1.026/1.297/1.928/0.266 ms
dadi@RogStrix:~$ traceroute 10.5.16.152
traceroute to 10.5.16.152 (10.5.16.152), 30 hops max, 60 byte packet
 1  10.5.16.152 (10.5.16.152)  1.021 ms  0.964 ms  0.944 ms
dadi@RogStrix:~$
```

(c) ping and traceroute to 10.5.16.152

```
250 7.578634976   10.5.16.225    10.5.16.152    ICMP   100 Echo (ping) request  id=0x666c, seq=4/1024, ttl=64 (reply in 251)
251 7.579828951   10.5.16.152    10.5.16.225    ICMP   100 Echo (ping) reply    id=0x666c, seq=4/1024, ttl=64 (request in 250)
302 8.580073819   10.5.16.225    10.5.16.152    ICMP   100 Echo (ping) request  id=0x666c, seq=5/1280, ttl=64 (reply in 303)
303 8.581190651   10.5.16.152    10.5.16.225    ICMP   100 Echo (ping) reply    id=0x666c, seq=5/1280, ttl=64 (request in 302)
358 9.581681463   10.5.16.225    10.5.16.152    ICMP   100 Echo (ping) request  id=0x666c, seq=6/1536, ttl=64 (reply in 359)
359 9.583055953   10.5.16.152    10.5.16.225    ICMP   100 Echo (ping) reply    id=0x666c, seq=6/1536, ttl=64 (request in 358)
411 10.583508602  10.5.16.225    10.5.16.152    ICMP   100 Echo (ping) request  id=0x666c, seq=7/1792, ttl=64 (reply in 412)
412 10.584807993  10.5.16.152    10.5.16.225    ICMP   100 Echo (ping) reply    id=0x666c, seq=7/1792, ttl=64 (request in 411)
467 11.585125719  10.5.16.225    10.5.16.152    ICMP   100 Echo (ping) request  id=0x666c, seq=8/2048, ttl=64 (reply in 468)
468 11.586272586  10.5.16.152    10.5.16.225    ICMP   100 Echo (ping) reply    id=0x666c, seq=8/2048, ttl=64 (request in 467)
588 13.992303413  10.5.16.152    10.5.16.225    ICMP   104 Destination unreachable (Port unreachable)
589 13.992303614  10.5.16.152    10.5.16.225    ICMP   104 Destination unreachable (Port unreachable)
590 13.992303664  10.5.16.152    10.5.16.225    ICMP   104 Destination unreachable (Port unreachable)
591 13.992303704  10.5.16.152    10.5.16.225    ICMP   104 Destination unreachable (Port unreachable)
592 13.992303754  10.5.16.152    10.5.16.225    ICMP   104 Destination unreachable (Port unreachable)
593 13.992303804  10.5.16.152    10.5.16.225    ICMP   104 Destination unreachable (Port unreachable)
```

(d) "ping" and "traceroute" captured in Wireshark.

```
dadi@RogStrix:~$ ping 19.168.1.100
PING 19.168.1.100 (19.168.1.100) 56(84) bytes of data.
^C
--- 19.168.1.100 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2068ms
```

(e) ping to unreachable host(19.168.1.100

```
Wireshark · Packet 386 · any
 Frame 386: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
 Linux cooked capture v1
 Internet Protocol Version 4, Src: 10.5.16.225, Dst: 192.168.1.100
 Internet Control Message Protocol
   Type: 8 (Echo (ping) request)
   Code: 0
   Checksum: 0x5ef5 [correct]
   [Checksum Status: Good]
   Identifier (BE): 26806 (0x68b6)
   Identifier (LE): 46696 (0xb668)
   Sequence Number (BE): 4 (0x0004)
   Sequence Number (LE): 1024 (0x0400)
  [No response seen]
   Timestamp from icmp data: Jan 17, 2025 23:05:39.295159000 IST
   [Timestamp from icmp data (relative): 0.000038465 seconds]
  Data (40 bytes)
```

(f) packet to unreachable host - no response

```
dadi@RogStrix:~$ traceroute 10.5.16.152
traceroute to 10.5.16.152 (10.5.16.152), 30 hops max, 60 byte packets
 1  10.5.16.152 (10.5.16.152)  1.158 ms  1.100 ms  1.080 ms
dadi@RogStrix:~$ traceroute 19.168.1.100
traceroute to 19.168.1.100 (19.168.1.100), 30 hops max, 60 byte packets
 1  _gateway (10.5.16.2)  0.940 ms  0.871 ms  0.849 ms
 2  10.120.2.33 (10.120.2.33)  0.824 ms  0.806 ms  0.789 ms
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
dadi@RogStrix:~$
```

(g) traceroute to 10.5.16.152(reachable host) and 19.168.1.100(unreachable host)

```
 334 8.910315251   10.5.16.225   192.168.1.100  ICMP  100 Echo (ping) request  id=0x68b6, seq=2/512, ttl=64 (no response found!)
 358 9.934329452   10.5.16.225   192.168.1.100  ICMP  100 Echo (ping) request  id=0x68b6, seq=3/768, ttl=64 (no response found!)
 386 10.958283607  10.5.16.225   192.168.1.100  ICMP  100 Echo (ping) request  id=0x68b6, seq=4/1024, ttl=64 (no response found!)
 416 11.982222360  10.5.16.225   192.168.1.100  ICMP  100 Echo (ping) request  id=0x68b6, seq=5/1280, ttl=64 (no response found!)
 457 13.006216150  10.5.16.225   192.168.1.100  ICMP  100 Echo (ping) request  id=0x68b6, seq=6/1536, ttl=64 (no response found!)
 507 14.030273223  10.5.16.225   192.168.1.100  ICMP  100 Echo (ping) request  id=0x68b6, seq=7/1792, ttl=64 (no response found!)
 530 15.054249130  10.5.16.225   192.168.1.100  ICMP  100 Echo (ping) request  id=0x68b6, seq=8/2048, ttl=64 (no response found!)
 630 18.009609548  10.5.16.225   172.16.1.180   ICMP  114 Destination unreachable (Port unreachable)
 636 18.013419421  127.0.0.1     127.0.0.53     ICMP  125 Destination unreachable (Port unreachable)
 640 18.013931872  127.0.0.1     127.0.0.53     ICMP  125 Destination unreachable (Port unreachable)
 929 23.008794465  10.5.16.225   172.16.1.164   ICMP  114 Destination unreachable (Port unreachable)
1326 33.328008764  127.0.0.1     127.0.0.53     ICMP  125 Destination unreachable (Port unreachable)
1689 43.032619580  127.0.0.1     127.0.0.53     ICMP  125 Destination unreachable (Port unreachable)
1691 43.032668531  127.0.0.1     127.0.0.53     ICMP  125 Destination unreachable (Port unreachable)
2125 53.039723445  127.0.0.1     127.0.0.53     ICMP  125 Destination unreachable (Port unreachable)
2312 57.655258556  10.5.16.225   172.16.1.164   ICMP  114 Destination unreachable (Port unreachable)
2811 63.057374349  127.0.0.1     127.0.0.53     ICMP  125 Destination unreachable (Port unreachable)
3626 78.061901225  10.5.16.225   172.16.1.164   ICMP  114 Destination unreachable (Port unreachable)
3631 78.064093685  127.0.0.1     127.0.0.53     ICMP  125 Destination unreachable (Port unreachable)
3870 83.067729060  127.0.0.1     127.0.0.53     ICMP  125 Destination unreachable (Port unreachable)
4501 93.076963307  10.5.16.225   172.16.1.164   ICMP  114 Destination unreachable (Port unreachable)
4505 93.077898594  127.0.0.1     127.0.0.53     ICMP  125 Destination unreachable (Port unreachable)
4678 98.082379378  127.0.0.1     127.0.0.53     ICMP  125 Destination unreachable (Port unreachable)
5676 119.869350977 10.5.16.152   10.5.16.225    ICMP  104 Destination unreachable (Port unreachable)
5677 119.869351318 10.5.16.152   10.5.16.225    ICMP  104 Destination unreachable (Port unreachable)
5678 119.869351438 10.5.16.152   10.5.16.225    ICMP  104 Destination unreachable (Port unreachable)
5679 119.869351548 10.5.16.152   10.5.16.225    ICMP  104 Destination unreachable (Port unreachable)
5680 119.869351658 10.5.16.152   10.5.16.225    ICMP  104 Destination unreachable (Port unreachable)
5681 119.869351778 10.5.16.152   10.5.16.225    ICMP  104 Destination unreachable (Port unreachable)
6454 142.012758266 10.5.16.2     10.5.16.225    ICMP   72 Time-to-live exceeded (Time to live exceeded in transit)
6455 142.012758446 10.5.16.2     10.5.16.225    ICMP   72 Time-to-live exceeded (Time to live exceeded in transit)
6456 142.012758496 10.120.2.33   10.5.16.225    ICMP   72 Time-to-live exceeded (Time to live exceeded in transit)
6457 142.012758546 10.5.16.2     10.5.16.225    ICMP   72 Time-to-live exceeded (Time to live exceeded in transit)
6458 142.012758587 10.120.2.33   10.5.16.225    ICMP   72 Time-to-live exceeded (Time to live exceeded in transit)
6459 142.012758637 10.120.2.33   10.5.16.225    ICMP   72 Time-to-live exceeded (Time to live exceeded in transit)
6869 151.613305441 10.255.1.3    10.5.16.225    ICMP  104 Time-to-live exceeded (Time to live exceeded in transit)
6870 151.621389373 10.255.1.3    10.5.16.225    ICMP  104 Time-to-live exceeded (Time to live exceeded in transit)
6871 151.644705223 10.255.1.3    10.5.16.225    ICMP  104 Time-to-live exceeded (Time to live exceeded in transit)
7025 156.088737425 10.5.16.225   172.16.1.180   ICMP  114 Destination unreachable (Port unreachable)
7028 156.092843200 127.0.0.1     127.0.0.53     ICMP  125 Destination unreachable (Port unreachable)
```

(h) traceroute to reachable and unreachable hosts

Figure 15: ICMP Packets for Ping/Traceroute.

For the first traceroute to the reachable host `10.5.16.152`, the packets were successfully routed to the destination in the first hop. This indicates that the destination IP is directly accessible on the local network. The ICMP Echo Request packets sent from the host were followed by the ICMP Echo Reply packets from the destination with minimal latency, confirming a direct and fast connection.

For the second traceroute to the unreachable host `19.168.1.100`, the process initially passed through the local gateway (`10.5.16.2`) and the first two hops responded successfully. However, after the second hop, all subsequent hops showed no response, marked by `* * *`. This suggests that the destination host is unreachable, either due to non-existence in the network, a firewall blocking ICMP replies, or a routing issue preventing the packets from reaching the destination. In Wireshark, while the ICMP Echo Request packets were sent, no ICMP Time Exceeded or Echo Reply packets were received beyond the second hop. This absence of responses indicates that the packets did not proceed beyond the first few hops, likely due to network or firewall filtering mechanisms.